EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mark Pratt on 9/29/2010.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 3/22/2010 has been entered.

Please amend the application as follows:

In the claims:

1. (Currently Amended) A content distribution server that encrypts a content and distributes the encrypted content to content output apparatuses connected to the content distribution server via a network, each of the content output apparatuses decrypting the encrypted content and outputting the decrypted content, the content distribution server comprising:

a key information storage unit, the key information storage unit being a hardware device and operable to hold a node encryption key group that is a set of node encryption keys which are previously assigned to the content output apparatuses using a predetermined key assignment method;

an encryption key group selection unit operable to select, from among the node encryption key group, at least one node encryption key as a selected node encryption key group;

a content decryption key selection unit operable to generate an encrypted content decryption key group that includes at least one encrypted content decryption key obtained by encrypting a previously given content decryption key using the at least one node encryption key in the selected node encryption key group;

a content receiving unit operable to receive a content via the network;

an encryption unit operable to encrypt the content using a content encryption key which is previously given as a pair with the content decryption key; and

a transmission unit operable to distribute the encrypted content and the encrypted content decryption key group to the content output apparatuses;

wherein the key assignment method has a tree structure in which a plurality of content output apparatuses serve as nodes, and includes:

classifying the nodes into a plurality of levels from a 0^{th} level through an nth level, n being 1 or a larger natural number; and

selecting, as terminal nodes in the tree structure, nodes each of which does not have a child node, from among the nodes, and

said encryption key group selection unit selects the selected node encryption key group so that the selected node encryption key group includes at least one node encryption key that is set for a terminal node and at least one node encryption key that is set for a node other than the terminal nodes by randomly selecting a node encryption key that is set for a terminal node among the terminal nodes and then further selecting a node encryption key assigned to a content output apparatus to which the selected node encryption key is not assigned.

29. (Currently Amended) A non-transitory computer-readable recording medium on which a program is recorded, the program being used for a content distribution server that encrypts a content and distributes the encrypted content to content output apparatuses connected to the content distribution server via a network, each of the content output apparatuses decrypting the encrypted content and outputting the decrypted content, the program comprising:

holding a node encryption key group that is a set of node encryption keys which are previously assigned to the content output apparatuses using a predetermined key assignment method;

selecting, from among the node encryption key group, at least one node encryption key as a selected node encryption key group;

generating an encrypted content decryption key group that includes at least one encrypted content decryption key obtained by encrypting a previously given content decryption key using said at least one node encryption key in the selected node encryption key group;

receiving a content via the network;

encrypting the content using a content encryption key which is previously given as a pair with the content decryption key; and

distributing the encrypted content and the encrypted content decryption key group to the content output apparatuses,

wherein the key assignment method has a tree structure in which a plurality of content output apparatuses serve as nodes, and includes:

classifying the nodes into a plurality of levels from a 0^{th} level to an nth level, n being 1 or a larger natural number; and

selecting, as terminal nodes in the tree structure, nodes each of which does not have a child node, from among the nodes, and

said encryption key group selection unit selects the selected node encryption key group so that said selected node encryption key group includes at least one node

encryption key that is set for a terminal node and at least one node encryption key that is set for the selected terminal node and node encryption key that is set for a node other than the terminal nodes by randomly selecting a node encryption key that is set for a terminal node among terminal nodes and then further selecting a node encryption key assigned to a content output apparatus to which the selected node encryption key is not assigned.

Reasons for Allowance

The following is an examiner's statement of reasons for allowance:

The closest prior art teaches content encryption and distribution using key trees, key groups, and use of multiple keys to encrypt the content key such that each authorized terminal can decrypt the content key using a key assigned thereto. However, the closest prior art fails to disclose that the selected encryption key group, used to encrypt the content key using multiple keys, is performed by randomly selecting a node encryption key set for a terminal node and selecting another node encryption key that is not assigned to that terminal node.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEFFREY D. POPHAM whose telephone number is (571)272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jeffrey D Popham
Examiner
Art Unit 2437

/Jeffrey D Popham/
Examiner, Art Unit 2437